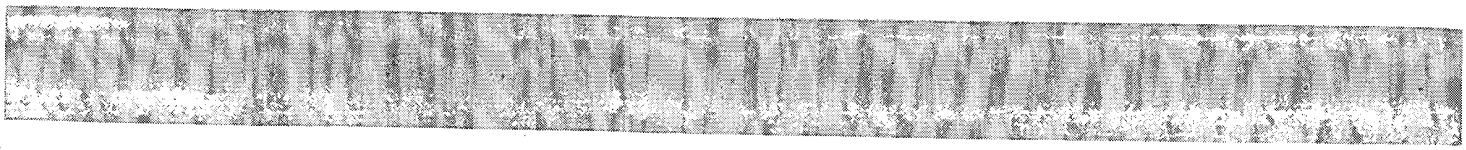
Control system object manager infrastructure for power plant control

Patent Number: DE19520744
Publication date: 1996-12-12
Inventor(s): FRITZ PETER (DE); WALZ HORST (DE); GLASER MARTIN DIPL ING (DE)
Applicant(s):: SIEMENS AG (DE)
Requested Patent: ☐ DE19520744
Application DE19951020744 19950607
Priority Number(s): DE19951020744 19950607
IPC Classification: G05B15/00 ; G05B9/03 ; H02J13/00 ; G06F19/00 ; H02B15/00
EC Classification: G05B19/418N, H02B15/00
Equivalents:

Abstract

The infrastructure (2) is used for a control system with a number of monitoring devices with data processing components, distributed at different monitoring points within the power plant and incorporates a number of distributed object manager components (4,..16), each having at least one object manager, with incorporated redundancy. The infrastructure monitors the operating condition of each redundant object manager component (10a,10b,12a,12b), or object manager (22a,22b, 24a,24b), with access to all other object manager components.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 195 20 744 C 2**

(51) Int. Cl.[6]:
G 05 B 15/00
G 05 B 9/03
H 02 J 13/00
G 06 F 19/00

(21) Aktenzeichen: 195 20 744.0-51
(22) Anmeldetag: 7. 6. 95
(43) Offenlegungstag: 12. 12. 96
(45) Veröffentlichungstag der Patenterteilung: 30. 9. 99

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Siemens AG, 80333 München, DE

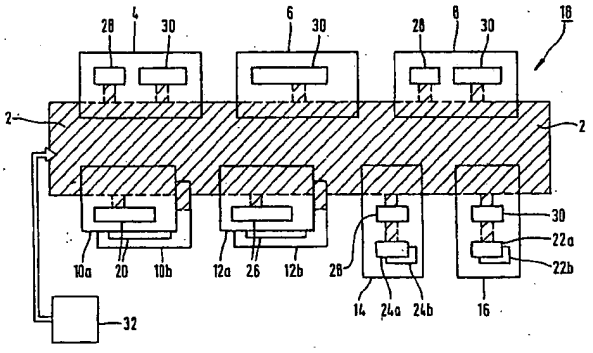
(72) Erfinder:
Walz, Horst, Dipl.-Inform., 75334 Straubenhardt, DE; Fritz, Peter, Dipl.-Inform., 76185 Karlsruhe, DE; Glaser, Martin, Dipl.-Ing., 76698 Ubstadt-Weiher, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

EP 06 04 091 A2
WO 95 30 937
net 40, 1986, H. 9, S. 338-342;
CH-Z.: Europhysics Conference on Control Systems for Experimental Physics, Proceedings (CERN 90-08)
Villars sur Ollon, Switzerland, 28.Sept. - 2.Oct. 1987, S. 15-20, Published: CERN, Geneva, Switzerland;
Elektronik 7/ 31.3.1989, S. 52-58;
Elektronik 25/ 1994, S. 58-64;

(54) Infrastruktur für ein System von verteilten Objektmanager-Komponenten

(57) Infrastruktur (2) für ein System von verteilten Objektmanager-Komponenten (4 bis 16), insbesondere für ein Leitsystem einer Kraftwerksanlage, mit einer Anzahl von rechnergestützten Objektmanager-Komponenten, die jeweils mindestens einen Objektmanager ausführen, wobei für redundant ausgeführte Objektmanager-Komponenten (10a, 10b, 12a, 12b) oder Objektmanager (22a, 22b, 24a, 24b) der Zustand "prozeßführend" und entsprechend "nicht-prozeßführend" überwacht und für alle übrigen Objektmanager-Komponenten (4, 6, 8, 14, 16) zugänglich ist.



DE 195 20 744 C 2

DE 195 20 744 C 2

Beschreibung

Die Erfindung bezieht sich auf eine Infrastruktur für ein System von verteilten Objektmanager-Komponenten, insbesondere für ein Leitsystem einer Kraftwerksanlage, mit einer Anzahl von rechnergestützten Objektmanager-Komponenten.

In einer Kraftwerksanlage sollen Überwachungseinrichtungen die aktuellen Betriebszustände der Anlage erkennbar machen und Abweichungen von einem Sollzustand melden. Dazu ist eine umfangreiche Meßwerterfassung der Betriebszustände aller Anlagenteile, eine umfangreiche und der Komplexität der Anlage gerecht werdende Meßwertbewertung und eine unter hoher Informationsverdichtung visualisiert aufbereitete Statusanzeige für die Betriebszustände der Anlagenteile erforderlich.

Diese vorstehend genannten Aufgaben soll ein Leitsystem erfüllen. Bedingt durch die hohe Komplexität solcher technischen Anlagen muß ein solches Leitsystem einfach und geradlinig strukturiert sein. Dies bedeutet zum einen, daß Anlagenteile mittels des Leitsystems überwachbar und einstellbar sind und zum anderen, daß neue und/oder überarbeitete und geänderte Kontroll-, Einstell- und/oder Auswerteoptionen in einfacher Weise in das bestehende Leitsystem und seine Architektur integrierbar sind.

Aus net 40 (1986), Heft 9, Seiten 338–342, insbesondere Bild 2, ist ein "Ringnetz mit Token Access" bekannt. Bild 3 zeigt die Möglichkeit, einen zusätzlichen gegenläufigen Ring zu integrieren.

Aus Elektronik 7/31.3.1989, Seiten 52–58, insbesondere Bilder 4 und 5, sind lokale Netze mit "Ringstruktur" und "Doppelringstruktur" bekannt. Als Zugriffsverfahren für lokale Netze sind insbesondere von Seite 53, dritter Absatz, das "Token-Ring-" und das "Token-Bus-Verfahren" bekannt.

Aus Europhysics Conference on Control Systems for Experimental Physics, Proceedings (CERN 90-08), Villars-sur-Ollon, Switzerland, 28. Sept. – 2. Oct. 1987, Seiten 15–20, published: CERN, Geneva, Switzerland 1990, vergleiche insbesondere Fig. 2, ist ein Steuer- und Regelungssystem mit einem "N-zu-N Token Ringnetz" bekannt.

Aus EP 0 604 091 A2, insbesondere Fig. 10, ist ein "Ringnetz" bekannt. Außerdem ist insbesondere aus Fig. 9 ein "Server" bekannt.

Aus Elektronik 25/1994, Seiten 58–64, vergleiche insbesondere Seite 59, rechte Spalte, ist das "Client-Server-Konzept" bekannt.

In der älteren Anmeldung WO 95/30937 ist ein Leitsystem, insbesondere ein rechnergestütztes Leitsystem, vorgeschlagen, bei dem eine hohe Konfigurierbarkeit einer die Meßwerte be- und auswertenden Ebene innerhalb des Leitsystems gegeben ist. Dies wird im einzelnen dadurch erreicht, daß die Leitebene modular aufgebaut ist und mehrere Funktionsbausteine umfaßt, die entsprechend ihrer jeweiligen Funktion Eingangswerte verarbeiten und unter Berücksichtigung einer Anzahl von zu lösenden technischen Anwendungen untereinander verknüpfbar sind. Aufgrund dieses modularen Aufbaus der Leitebene und ihrer Systeme sind eine nahezu beliebige Strukturierbarkeit und graphische Konfigurierbarkeit des Leitsystems in dieser Ebene gegeben. Es können jederzeit Funktionsbausteine modifiziert, ergänzt, weggenommen oder neu verknüpft werden, um eine zu lösende technische Anwendung, wie z. B. die Prozeßführung bestimmter Anlagenteile, die Prozeßinformation, die Kenngrößenberechnung oder die Bilanzierung, durchführen zu können. Die dabei verarbeiteten Eingangswerte können die unmittelbar von der Automatisierungsebene erhaltenen Meßwerte, bereits mit einer Zugehörigkeitsfunktion bewertete Meßwerte, Zwischenresultate anderer Funktionsbausteine und über die Betriebsführungsebene vorgebbare projektierbare Parameter sein.

Bei einem solchen meist rechnergestützten Leitsystem ist es wünschenswert, wenn die Leitebene und die mit der Leitebene verbundenen Ebenen innerhalb einer gemeinsamen Systemumgebung, einer sogenannten Infrastruktur, geführt sind. Hierzu ist es bekannt, ein Betriebssystem, vorzugsweise ein handelsübliches Betriebssystem, wie z. B. UNIX oder OS 2, zu verwenden, das die Betriebsführungsebene, die Leitebene und die Automatisierungsebene sowie einen Datentransfer zwischen diesen Ebenen unterhält. Bei solchen Betriebssystemen ist es darüber hinaus wünschenswert, wenn die freie Verknüpfbarkeit der in der Leitebene angeordneten Funktionsbausteine unterstützt wird, und wenn eine weitgehende Unabhängigkeit des Leitsystems von der Innovationsgeschwindigkeit der Rechner-Hardware erreicht wird.

Derzeit handelsübliche Betriebssysteme, wie z. B. UNIX oder OS 2, sind jedoch überfordert, wenn es im Rahmen einer Infrastruktur für ein System von verteilten Objektmanager-Komponenten darum geht, beispielsweise ein aus einer Anzahl von rechnergestützten Objektmanager-Komponenten bestehendes verteiltes System hochzufahren. Eine nicht zufriedenstellende derzeitige Lösung sieht hierzu einen übergeordneten Rechner vor, der zu Beginn des Anlaufs die Informationen über die gesamte Konfiguration aller existierenden Objektmanager-Komponenten kennt. Bedingt durch die Komplexität einer Kraftwerksanlage kommt es zu Störungen, wenn beispielsweise der übergeordnete Rechner gestört ist, oder wenn die Datenverbindungen zu diesem übergeordneten Rechner gestört sind, oder wenn sich an der Gesamtkonfiguration noch kurzfristig vor dem Anlaufen etwas geändert hat und diese Änderungen noch nicht zu Beginn des Anlaufs berücksichtigt worden sind.

Weitere Probleme treten auf, wenn einzelne Objektmanager-Komponenten redundant ausgeführt sind. Die Probleme werden durch die Tatsache verursacht, daß der übergeordnete Rechner zu jeder Zeit Kenntnis davon haben muß, welche Objektmanager-Komponente prozeßführend und welche Objektmanager-Komponente nicht-prozeßführend ist.

Der Erfindung liegt daher die Aufgabe zugrunde eine Infrastruktur für ein System von verteilten Objektmanager-Komponenten anzugeben, mit der jederzeit sichergestellt ist, daß eine störungsfrei vorliegende Information über den Zustand von redundant ausgeführten Objektmanager-Komponenten vorliegt.

Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß eine Infrastruktur für ein System von verteilten Objektmanager-Komponenten mit einer Anzahl von rechnergestützten Objektmanager-Komponenten, die jeweils mindestens einen Objektmanager ausführen, vorgesehen ist, wobei für redundant ausgeführte Objektmanager-Komponenten oder Objektmanager der Zustand "prozeßführend" und entsprechend "nicht-prozeßführend" überwachbar und für alle übrigen Objektmanager-Komponenten zugänglich ist.

Hierbei wird unter einer Objektmanager-Komponente beispielsweise eine Workstation, ein Personal-Computer, Automatisierungssysteme, wie z. B. die Siemens-Siematic S5 und S7, oder vergleichbare rechnergestützte Einrichtungen verstanden. Unter einem Objektmanager werden insbesondere bei einer Kraftwerksanlage die folgenden Komponenten verstanden. Es sind dies das Man-Machine-Interface, das Archiv, die Protokolliste, die Verarbeitungseinrichtung für die Bausteintechnik, eine Datenbank für Beschreibungs-, Symptom- und Diagnosetexte und ein sogenannter AS-Repräsentant, der das Automatisierungssystem, also die Schnittstelle zwischen Kraftwerksprozeß und Datenverar-

beitung, stützt.

Auf diese Weise ist es möglich, daß jede Objektmanager-Komponente in Folge der entsprechenden Ausgestaltung der Infrastruktur Kenntnis über den aktuellen Redundanz-Zustand der am System beteiligten Objektmanager-Komponenten und Objektmanager hat. Fehler, die durch eine übergeordnete Überwachungsinstanz auftreten können, sind auf diese Weise eliminiert.

In vorteilhafter Weise kann ein Zustandübergang einer Objektmanager-Komponente oder eines Objektmanagers bei Vorliegen eines Ausfallereignisses selbsttätig erfolgen. Dies bedeutet insbesondere, daß die Infrastruktur eine für alle Objektmanager-Komponenten zugängliche Meldung in auf ebensolche Meldungen wartende Schnittstellen der Objektmanager-Komponenten schreibt.

In weiter zweckmäßiger Weise ist die Infrastruktur derart ertüchtigt, daß die Übermittlung eines datenlesenden Auftrages an den prozeßführenden Server erfolgt, und/oder das die Übermittlung eines datenschreibenden Auftrages an alle zueinander redundanten Objektmanager-Komponenten oder Objektmanager erfolgt. Auf diese Weise ist es gewährleistet, daß ein datenlesender Client unverzüglich bedient wird bzw. daß eine redundant ausgeführte, aber derzeit nicht-prozeßführende Objektmanager-Komponente oder Objektmanager jederzeit in der Lage ist, an die prozeßführende Stelle zu treten.

Eine weitere vorteilhafte Ausgestaltung der Erfindung sieht es vor, daß zum Aufdaten von Objektmanagern auf wiederanlaufenden redundanten Objektmanager-Komponenten der führende Server auf Auftrag ein konsistentes Abbild seiner Prozeßdaten erstellt und zum aufrufenden Client überträgt. Auf diese Weise enthält der auf der wiederanlaufenden redundanten Objektmanager-Komponente installierte Objektmanager nach definierter Aufforderung zu einem definierten Zeitpunkt alle für den Betrieb des Objektmanagers erforderliche Daten. Es entstehen also keine Datenlücken oder Fehler durch die Übermittlung nicht aktueller Prozeßdaten.

In besonders einfacher Weise läßt sich die Erfindung ausgestalten, wenn eine Objektmanager-Komponente oder ein Objektmanager in dem jeweiligen Server-Hauptteil eine Schnittstelle aufweist, die eine Änderung des Redundanz-Zustandes der entsprechenden Komponente oder des entsprechenden Objektmanagers erfaßt.

Ausführungsbeispiele der Erfindung werden anhand einer Zeichnung näher erläutert. Dabei zeigen:

Fig. 1 in schematischer Darstellung eine Infrastruktur für ein verteiltes System von Objektmanager-Komponenten;

Fig. 2 in schematischer Darstellung einen in die Infrastruktur eingebetteten Objektmanager;

Fig. 3 in schematischer Darstellung den Überwachungsmechanismus der gemäß **Fig.** 1 dargestellten Infrastruktur;

Fig. 4 in schematischer Darstellung den Überwachungsmechanismus gemäß **Fig.** 3 bei dem Ausfall einer Objektmanager-Komponente; und

Fig. 5 in schematischer Darstellung den Überwachungsmechanismus in der Infrastruktur gemäß den **Fig.** 3 und 4 in zwei Überwachungsebenen.

In den **Fig.** 1 bis 5 haben gleiche Teile die gleichen Bezugszeichen.

In der in **Fig.** 1 gezeigten schematischen Darstellung erkennt man die Infrastruktur **2** für ein verteiltes System **18** von Objektmanager-Komponenten **4** bis **16** als schraffiert unterlegte Fläche. Das System **18** ist als Leitsystem für eine Kraftwerksanlage vorgesehen. Die Objektmanager-Komponenten **4** bis **16** können Datenverarbeitungsanlagen beliebiger Art, wie z. B. Großrechner, Workstations, Personal-Computer und Host-Rechner jeglicher Art, sein. Auf den einzelnen Objektmanager-Komponenten **4** bis **16**, von denen die Komponenten **10a** und **10b** sowie **12a** und **12b** redundant ausgeführt sind, werden Objektmanager ausgeführt.

Unter Objekten werden Daten jeglicher Art, wie z. B. binäre Signale, hexadezimale Signale, wie z. B. Real-Werte, Integer-Werte, Boolean-Werte oder String-Ketten, verstanden. Objektmanager sind also solche hardwaremäßig oder auch softwaremäßig realisierte Einheiten, die Objekte beliebiger Art verwalten. Objektmanager sind beispielsweise das Man-Machine-Interface (MMI) **20**, das Archiv **22** zur Aufzeichnung der Geschichte des Kraftwerks (redundant ausgeführt als **22a** und **22b**), der Protokollverwalter **24** (ebenfalls redundant ausgeführt als **24a** und **24b**), der Verwalter **26** für die Datenverarbeitung der in Bausteintechnik vorgesehenen und hier nicht weiter dargestellten Leitebene, die Datenbank **28** für Beschreibungsdaten und der Repräsentant **30** des Automatisierungssystems. Wie beispielsweise anhand des Repräsentanten **30** des Automatisierungssystems gezeigt, kann ein Objektmanager auch auf mehreren Objektmanager-Komponenten, hier die Komponenten **4** bis **8** und **16**, gleichzeitig ausgeführt werden.

Beim Anlauf des Systems **18** werden von einer dezentral angeordneten Initialisierungsdatei **32** die Anlaufdaten in die Infrastruktur **2** eingegeben. Jeder der Objektmanager-Komponenten **4** bis **16** hat einen Teil seiner zur Verfügung stehenden Rechenleistung reserviert, um die Infrastruktur **2** in hardwaremäßig verschalteter Form oder auch in softwaremäßig installierter Form zu betreiben. Die Anlaufdaten der Initialisierungsdatei **32** enthalten einen dezentralen Algorithmus, nach dem in einer ersten Phase des Anlaufs die Objektmanager-Komponenten **4** bis **16** untereinander Kontakt aufnehmen und der Infrastruktur **2** und damit allen an der Infrastruktur **2** beteiligten Komponenten **4** bis **16** ihre lokal installierten Objektmanager **20** bis **30** bekannt. Nach dieser Kontaktaufnahme sind auf jeder Objektmanager-Komponente **4** bis **16** alle anlaufenden Objektmanager-Komponenten und alle dort existierenden Objektmanager bekannt.

In einer zweiten Phase werden mittels der Infrastruktur **2** auf den Objektmanager-Komponenten **4** bis **16** die lokal installierten Objektmanager **20** bis **30** gestartet. Die Infrastruktur **2** wartet ferner darauf, daß die Objektmanager **20** bis **30** ihre Verfügbarkeit als Server bekannt geben, und aktualisiert – auch wenn der Überwachungsmechanismus einen Abbruch eines Objektmanagers erkannt hat – den neuen Zustand zusammen mit einer detaillierten Adressinformation auf allen Objektmanager-Komponenten **4** bis **16**. In einer dritten Phase werden die Objektmanager **20** und **26** auf den redundant vorliegenden Objektmanager-Komponenten **10a**, **10b** bzw. **12a**, **12b** gestartet. Dabei datet sich der jeweils führende Redundanzpartner am allen Objektmanager-Komponenten **4** bis **16** gemeinsamen Anlaufprozeß auf und der oder die nicht führenden Objektmanager daten sich beim jeweils führenden Objektmanager auf.

Die Infrastruktur **2** unterstützt auch eine weitere Anlaufsituation, bei der sich eine abgebrochene Objektmanager-Komponente, beispielsweise die Komponente **6**, in ein etabliertes Teilsystem, bestehend aus den Komponenten **4**, **8** bis **16**, wieder eingliedert. Die sich eingliedernde Objektmanager-Komponente **6** stellt sich zunächst bei einer schon im Teilsystem etablierten Objektmanager-Komponente, beispielsweise der Komponente **8**, vor, indem die Objektmanager-Komponente **6** ihre lokal installierten Objektmanager, hier der Repräsentant **30** des Automatisierungssystems, mitteilt. Die lokale Infrastruktur der Objektmanager-Komponente **8**, dargestellt durch die schraffierte Fläche innerhalb des Symbols für die Objektmanager-Komponente **8**, macht die sich eingliedernde Objektmanager-Komponente **6** im etablierten Teilsystem bekannt. Die sich eingliedernde Ob-

jektmanager-Komponente **6** erhält von der Komponente **8**, bei der sie sich vorgestellt hat, die Informationen über die Zustände und Adressen der Objektmanager-Komponente **4**, **8** bis **16** des etablierten Teilsystems und der darauf installierten Objektmanager. Auf diese Weise wird die Objektmanager-Komponente **6** in das etablierte Teilsystem eingegliedert ohne daß eine übergeordnete Instanz, beispielsweise ein Leitrechner, vorgesehen ist, der die Konfiguration, Zustände und Adressen der übrigen Objektmanager-Komponenten kennt. Diese Informationen sind vielmehr auf jeder Objektmanager-Komponente **4** bis **16** im lokalen Teil der Infrastruktur **2** enthalten, so daß auch jede Änderung des Status einer Objektmanager-Komponente oder eines Objektmanagers allen Objektmanager-Komponenten unmittelbar zugänglich ist. Dies wirkt sich besonders vorteilhaft auf die Serverfunktionen der Objektmanager und auf die Kenntnis deren Verfügbarkeit im gesamten System **18** aus. In beiden Anlaufsituationen startet die Infrastruktur **2** die lokal installierten Objektmanager, in dem sie deren Inatialisierungsprozesse erzeugt. Objektmanager, die dem System **18** keine Serverleistung zur Verfügung stellen, sind mit diesem Schritt sofort verfügbar.

Der Abbruch eines Objektmanagers **20** bis **30** während des Anlaufs wirkt sich abhängig vom Vorhandensein einer Redundanz auf den Zustand der entsprechenden Objektmanager-Komponente **4** bis **16** aus: Bei vorhandener Redundanz werden die schon aktiven Objektmanager beendet und die Objektmanager-Komponente wird als "abgebrochen" für alle übrigen Objektmanager-Komponenten zugänglich markiert. Ohne vorhandene Redundanz wird der Anlauf der Objektmanager-Komponente fortgesetzt. Nur der vom Abbruch betroffene Objektmanager wird als "abgebrochen" markiert.

In **Fig.** 2 ist in schematischer Darstellung gezeigt, in welcher Weise ein Objektmanager, hier beispielsweise der Objektmanager **30**, aufgebaut und in die Infrastruktur **2** eingebunden ist. Im vorliegenden Fall weist der Objektmanager **30** zwei Client-Schnittstellen **32**, **34**, einen Init-Server **36**, einen Server-Hauptteil **38**, einen Server-Übertragungsteil **40** und einen Server **42** für Projektierungsdienste auf.

Über die Client-Schnittstellen **32**, **34**, die auch als Schnittstelle Client-Infrastruktur **2** bezeichnet werden kann, werden Aufträge über die Infrastruktur **2** an Server ausgegeben, und es können Antworten vom Server über die Infrastruktur **2** in der Schnittstelle empfangen werden. Hierbei kann die Schnittstelle als Mehrfachwartestelle ausgeführt sein, so daß es möglich ist, auf die Ergebnisse verschiedener Aufträge unabhängig voneinander warten zu können, was sich besonders vorteilhaft auf die Synchronisation von Datenaustauschvorgängen auswirkt.

Der Init-Server **36** wird beim Anlauf des Objektmanagers **30** aufgerufen. Dieser Init-Server **36** startet und überwacht alle weiteren Prozesse, die auf dem Objektmanager **30** ausgeführt werden. Der Init-Server **36** teilt allen übrigen Prozessen darüber hinaus wichtige Konfigurations- und Adressinformationen mit. Falls der Objektmanager **30** beendet werden soll, wird dies dem Init-Server **36** von der Infrastruktur **2** über ein entsprechendes Signal, beispielsweise ein UNIX-Signal, mitgeteilt. Das Beenden des Objektmanagers **30** wird der Infrastruktur **2** durch das Beenden des Init-Servers **36** mitgeteilt.

Der Server-Hauptteil **38** stellt dem Server für alle "Nutzfunktionen" des Objektmanagers **30** dar. Im Server-Hauptteil **38** ruft das Hauptprogramm nach der eigenen Initialisierung durch den Init-Server **36** eine Überwachungsfunktion auf. Diese Überwachungsfunktion wartet über die gesamte Lebensdauer des Server-Hauptteils **38** auf Client-Aufträge und ruft entsprechend dieser Aufträge Server-Funktionen auf, d. h. der Server-Hauptteil **38** wartet in einer Wartestelle in der Infrastruktur **2** auf entsprechende Client-Aufträge. Diese Funktion ist daher eine Art vorgeschobener Horchposten aus dem Objektmanager **30** heraus in die Infrastruktur **2**. Erst wenn der Server-Hauptteil **38** beendet wird, verläßt diese Funktion die Infrastruktur **2** und kehrt in das Hauptprogramm zurück.

Der Server-Übertragungsteil **40** stellt einen in den Prozeß des Objektmanagers **30** eingebundenen Funktionssatz dar, über den Server antworten (z. B. für kontinuierliche Aufträge) abgegeben werden. Der Server-Übertragungsteil **40** überträgt, falls sich ein Client über den Server-Hauptteil **38** angemeldet hat, die gewünschten Ereignisse oder sonstige Ereignisse von kontinuierlichen Aufträgen.

Der Server **42** für Projektierungsdienste wartet nach seiner Aktivierung auf Projektierungsaufträge und legt die Projektierungsinformation in eine Objektmanager spezifische Datenbasis ab oder gibt sie an die innerhalb des Objektmanagers **30** betroffenen Prozesse weiter.

Die Infrastruktur **2** überwacht und steuert die gesamte Kommunikation in einer Weise, daß jedes Objekt ein internes Kennzeichen und einen Ausprägungstyp umfaßt, anhand deren der Objektmanager, beispielsweise Objektmanager **30**, ermittelbar ist, der dieses Objekt verwaltet. Hierbei wird unter einem Objekt jede Information verstanden, die in einer Datenverarbeitungsanlage zur Kommunikation von Prozessen ausgetauscht oder übertragen wird. Mit dem Ausprägungstyp eines Objektes ist beispielsweise zunächst gemeint, ob dieses Objekt der verfahrenstechnischen Welt, der leittechnischen Welt oder der anlagentechnischen Welt zuzuordnen ist. Weiter beinhaltet der Ausprägungstyp eine Klassifizierung des Objekts nach seiner Aufgabenumgebung, beispielsweise kann ein Objekt Alarm- oder Toleranzmeldungen, Hardware-Gerätefehlern, Busfehlern oder Funktionsfehlern zugeordnet sein. Das interne Kennzeichen ist nicht gleichbedeutend mit dem Begriff "Adresse", weil das interne Kennzeichen keinerlei Ortsinformation über die Lage des Objektes besitzt. Darüber hinaus kann dem internen Kennzeichen nicht eindeutig eine Adresse zugeordnet werden, denn verschiedene Daten eines Objekts können von verschiedenen Objektmanagern **20** bis **30** verwaltet werden, die unter Umständen auf verschiedenen Objektmanager-Komponenten **4** bis **16** angesiedelt sind. Auf diese Weise ist mit besonders vorteilhafter Wirkung eine Adressierung von Objekten anhand ihrer Eigenschaften, d. h. eine assoziative Adressierung, möglich. Hierdurch vereinfacht sich die Projektierung, weil ganze Objekt-Klassen ausgewählt werden können, ohne daß deren Lage im einzelnen einem Objektmanager oder einer Objektmanager-Komponente bekannt sein müssen. So kann beispielsweise von dem Objektmanager **4**, dem Man-Machine-Interface, das Kommando abgesetzt werden "Suche Leittechnikfehler". Auf diese Weise sind in dem gesamten System **18** nur solche Objekte angesprochen, die gemäß ihres internen Kennzeichens und des Ausprägungstyps in die Signalklasse "Leittechnikfehler" hineinfallen.

Die Kommunikation im System **18** kann zum einen eine von einem Server-gesteuerte diskontinuierliche Kommunikation und zum anderen eine von einem Client-gesteuerte, kontinuierliche Kommunikation sein. Bei der Server-gesteuerten Kommunikation muß der Client den Umfang der Ergebnisse nicht kennen, Teilergebnisse können übertragen werden, wenn sie anfallen. Durch die Client-gesteuerte Kommunikation wird das gesamte Kommunikationsaufkommen im System **18** verringert, weil keine Auftragswiederholungen notwendig sind. Die Infrastruktur **2** ist hierbei derart konzipiert, daß bei dem Vorliegen eines Kommunikationsauftrages eines Clienten alle an diesem Auftrag betei-

ligten Server unmittelbar und nur einmalig zur Datenausgabe aufgefordert sind. Gleichzeitig kann mit einer solchen Aufforderung eine Synchronisationsaufforderung an alle beteiligten Server ergehen. Weiter kann in besonders zweckmäßiger Weise die Meldung des Vollzugs der Synchronisation an den Client erst dann ergehen, wenn die Bereitschaft zur Datenausgabe aller verfügbaren Server vorliegt, so daß auch hier das Kommunikationsaufkommen besonders gering ist, weil keine Nachfragen des Clients nach bestimmten Ergebnissen an einzelne Server ergehen.

Eine weitere vorteilhafte Ausgestaltung der Infrastruktur **2** sieht es vor, daß eine Wiederanmeldung eines noch anstehenden Auftrages eines Clienten bei einem wiederverfügbar gewordenen Server vorgesehen ist. Die Infrastruktur **2** stellt also Ressourcen bereit, die alle im System **18** eingegangenen Aufträge erfaßt und speichert, falls ein Server zur Auftragserledigung nicht verfügbar ist. Da die Infrastruktur gleichzeitig jede Zustandsänderung eines Servers bezüglich seiner Verfügbarkeit erfaßt, wird eine Auftragserledigung unmittelbar nach Wiederverfügbarkeit eines Servers "angemahnt".

Die Infrastruktur **2** ist weiter in der Lage einen Kommunikationsauftrag bezüglich der Parameterversorgung zu prüfen und den Auftrag bei fehlerhafter Parameterversorgung unter Angabe eines Fehlercodes abzulehnen. Auf diese Weise können beispielsweise Fehler vermieden werden, wenn bei der Suche nach einem Leittechnikfehler in der verfahrenstechnischen oder anlagentechnischen Welt gesucht wird. Ein solcher Fehler ist nur in der leittechnischen Welt zu finden, d. h. also bei den Datenquellen und Senken, die vom Ausprägungstyp her mit der Fehlerklasse übereinstimmen.

Hierbei kann das dynamische Verhalten der Erledigung eines Kommunikationsauftrages nachvollziehbar und verifizierbar sein. Eine solche Funktion kann beispielsweise über den Protokollverwalter **24** an die dem Man-Machine-Interface zugeordneten Drucker ausgegeben werden. Dies ist in der Projektierungsphase besonders bedeutsam, wenn man nachvollziehen will, welche Daten woher geladen wurden, und in welcher Weise daraus Ergebnisse berechnet wurden, und wohin die Ergebnisse gesendet wurden.

In **Fig.** 3 ist der Überwachungsmechanismus der Objektmanager-Komponenten **4** bis **16** in dem System **18** dargestellt. Der Mechanismus wird anhand der Objektmanager-Komponenten **4** bis **8** erläutert. Die Objektmanager-Komponente **6** arbeitet bei der Überwachung als Client für die Objektmanager-Komponente **8** und als Server für die Objektmanager-Komponente **4**. Die Objektmanager-Komponenten **4** bis **16** sind zur Überwachung ihres Zustandes in einem logischen Ring angeordnet, so daß keine übergeordnete Überwachungskomponente erforderlich ist. Die Überwachung erfolgt nach dem Client-Server Prinzip. Die als Client arbeitende Objektmanager-Komponente **6** sendet in definierten Zeitabständen ein Signal (Objekt) an die entsprechend als Server ausgebildete Objektmanager-Komponente **8**. Diese Komponente **8** sendet daraufhin ein "Lebenszeichen" an die Komponente **6**. In gleicher Weise erhält die Komponente **6** von der Komponente **4** in definierten Zeitabständen eine Aufforderung, ein "Lebenszeichen" zu senden. Zur Serversuche läuft auf allen Objektmanager-Komponenten **4** bis **16** der gleiche Algorithmus ab, beispielsweise können die Objektmanager-Komponenten **4** bis **16** ihren Überwacher und den zu Überwachenden anhand der alphabetischen Reihenfolge ihrer Benennung ermitteln.

In **Fig.** 4 ist eine gegenüber **Fig.** 3 geringfügig modifizierte Konfiguration des Systems **18** dargestellt. Hier sind die Objektmanager-Komponenten **6** und **10a** ausgefallen. Der Server der ausgefallenen Objektmanager-Komponente **6** kennt die Konfiguration dieser Komponente und teilt über die Infrastruktur **2** den verbleibenden Objektmanager-Komponenten alle mit der Objektmanager-Komponente ausgefallenen Objektmanager mit. Dies ist im vorliegenden Fall der auf der Objektmanager-Komponente **6** durchgeführte Objektmanager **30**. Gemäß der vorgegebenen Algorithmus hat die Objektmanager-Komponente **4** nun nicht die Objektmanager-Komponente **6** als Server, sondern die Objektmanager-Komponente **8**, so daß die im verbleibenden System aktiven Objektmanager-Komponenten **4**, **8** bis **16** wieder einen logischen Überwachungsring bilden. Will sich die Objektmanager-Komponente **6** wieder in das System eingliedern, meldet sie sich bei der Objektmanager-Komponente **8** an, gibt ihre lokal installierten Objektmanager, hier der Objektmanager **30**, bekannt und erfährt von der Objektmanager-Komponente **8** die Konfiguration und Zustände aller übrigen Objektmanager-Komponenten. Dies ist durch die gestrichelten Pfeile **44** symbolisiert.

Ein weiterer Spezielfall ist für die Objektmanager-Komponenten **10a** und **10b** dargestellt. Diese Komponente ist redundant ausgeführt. Im gezeigten Fall ist die Komponente **10a** ausgefallen. Der Server dieser Komponente **10a** kennt die Konfiguration dieser Komponente und die auf dieser Komponente lokal installierten Objektmanager, hier das Man-Machine-Interface **20**, und teilt den übrigen Objektmanager-Komponenten, die mit der Objektmanager-Komponente ausgefallenen Objektmanager mit. Hierbei ist es die Infrastruktur **2**, die ein für alle Objektmanager-Komponenten zugängliches Ereignis generiert, das insbesondere den verbleibenden Komponenten mitteilt, ob eine Objektmanager-Komponente "prozeßführend" oder "nicht-prozeßführend" ist bei redundanter Ausführung der jeweiligen Komponente.

Nach dem Ausfall der Komponente **10a** erfolgt der Zustandsübergang der Objektmanager-Komponente von "nicht-prozeßführend" nach "prozeßführend" der Komponente **10b** selbsttätig. Hierbei kann es weiter vorgesehen sein, daß zum Aufdaten von Objektmanagern auf wiederanlaufenden redundanten Objektmanager-Komponenten der prozeßführende Server auf Auftrag ein konsistendes Abbild seiner Prozeßdaten erstellt und zum aufrufenden Client, hier der Server der ausgefallenen Objektmanager-Komponente **10a**, überträgt. Um den Redundanz-Zustand einer Objektmanager-Komponente für die übrigen Komponenten zugänglich zu machen, ist es vorgesehen, daß jede Objektmanager-Komponente **4** bis **16** oder jeder Objektmanager in dem entsprechenden Server-Hauptteil **38** eine Schnittstelle aufweist, die eine Änderung des Redundanz-Zustandes der jeweils anderen Objektmanager-Komponenten oder Objektmanager erfaßt.

Insbesondere für die Handhabung einer sicheren Datenübertragung von redundant ausgeführten Objektmanager-Komponenten ist die Infrastruktur **2** derart ausgestaltet, daß die Übermittlung eines datenlesenden Auftrages selbsttätig an den prozeßführenden Server erfolgt. Hierzu dient beispielsweise der Eintrag in der vorstehend genannten Schnittstelle bezüglich des Zustands einer Objektmanager-Komponente oder eines Objektmanagers. Gleichzeitig sorgt die Infrastruktur **2** dafür, daß die Übermittlung eines datenschreibenden Auftrages an alle zueinander redundanten Objektmanager-Komponenten oder Objektmanager erfolgt, so daß der nicht prozeßführende Teil jederzeit in der Lage ist, die Prozeßführung zu übernehmen.

Auch der logische Ring zur Überwachung der Objektmanager-Komponenten **4** bis **16** schließt sich bei dem Ausfall der Objektmanager-Komponente **10a** selbsttätig, weil die Objektmanager-Komponenten **4** und **12a**, **12b** automatisch auf die redundante Objektmanager-Komponente **10b** um-

schalten, die ihren Zustand von "nicht-prozeßführend" nach "prozeßführend" geändert hat, wie dies die Pfeile **46**, **48** symbolisieren.

In **Fig.** 5 ist nochmals der logische Ring zur Überwachung der Objektmanager-Komponenten **4** bis **16** schematisch dargestellt. Hierbei soll deutlich gemacht werden, daß die Überwachung in zwei Überwachungsebenen erfolgt. In der ersten Überwachungsebene überwachen sich die Objektmanager-Komponenten **4** bis **16** selbsttätig im gemäß **Fig.** 3 beschriebenen Ring. Dies ist in **Fig.** 5 durch die Pfeilverbindungen von Objektmanager-Komponente zu Objektmanager-Komponente symbolisiert.

An der hier ausgewählten Objektmanager-Komponente **14** ist die zweite Überwachungsebene schematisch dargestellt. Innerhalb einer Objektmanager-Komponente werden zyklisch wiederkehrend die Zustände der einzelnen lokal installierten Objektmanager, hier der redundant ausgeführte Protokollverwalter **24a**, **24b** und die Datenbank **28** für Beschreibungsdaten, überwacht. Auf diese Weise ist eine Entkopplung der Überwachungsprozesse für Objektmanager-Komponenten und Objektmanager erreicht, so daß beispielsweise nach dem Ausfall eines einzelnen Objektmanagers nicht die gesamte Objektmanager-Komponente als ausgefallen gemeldet werden muß.

Patentansprüche

1. Infrastruktur (**2**) für ein System von verteilten Objektmanager-Komponenten (**4** bis **16**), insbesondere für ein Leitsystem einer Kraftwerksanlage, mit einer Anzahl von rechnergestützten Objektmanager-Komponenten, die jeweils mindestens einen Objektmanager ausführen, wobei für redundant ausgeführte Objektmanager-Komponenten (**10a**, **10b**, **12a**, **12b**) oder Objektmanager (**22a**, **22b**, **24a**, **24b**) der Zustand "prozeßführend" und entsprechend "nicht-prozeßführend" überwacht und für alle übrigen Objektmanager-Komponenten (**4**, **6**, **8**, **14**, **16**) zugänglich ist.
2. Infrastruktur (**2**) nach Anspruch 1, dadurch gekennzeichnet, daß ein Zustandsübergang einer Objektmanager-Komponente (**10a**, **10b**, **12a**, **12b**) oder eines Objektmanagers (**22a**, **22b**, **24a**, **24b**) bei Vorliegen eines Ausfallereignisses selbsttätig erfolgt.
3. Infrastruktur (**2**) nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Übermittlung eines datenlesenden Auftrages an den jeweils prozeßführenden Server einer Objektmanager-Komponente oder eines Objektmanagers erfolgt.
4. Infrastruktur (**2**) nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Übermittlung eines datenschreibenden Auftrages an alle zueinander redundanten Objektmanager-Komponenten (**10a**, **10b**, **12a**, **12b**) oder Objektmanager (**22a**, **22b**, **24a**, **24b**) erfolgt.
5. Infrastruktur (**2**) nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß zum Aufdaten von Objektmanagern (**20**, **26**) auf wiederanlaufenden redundanten Objektmanager-Komponenten der führende Server auf Auftrag ein konsistentes Abbild seiner Prozeßdaten erstellt und zum aufrufenden Client überträgt.
6. Infrastruktur (**2**) nach Anspruch **5**, dadurch gekennzeichnet, daß eine Objektmanager-Komponente (**10a**, **10b**, **12a**, **12b**) oder ein Objektmanager (**22a**, **22b**, **24a**, **24b**) in einem Server-Hauptteil (**38**) eine Schnittstelle (**36**) aufweist, die eine Änderung des Redundanz-Zustandes erfaßt.

Hierzu 5 Seite(n) Zeichnungen

Nummer: DE 195 20 744 C2
Int. Cl.[6]: G 05 B 15/00
Veröffentlichungstag: 30. September 1999

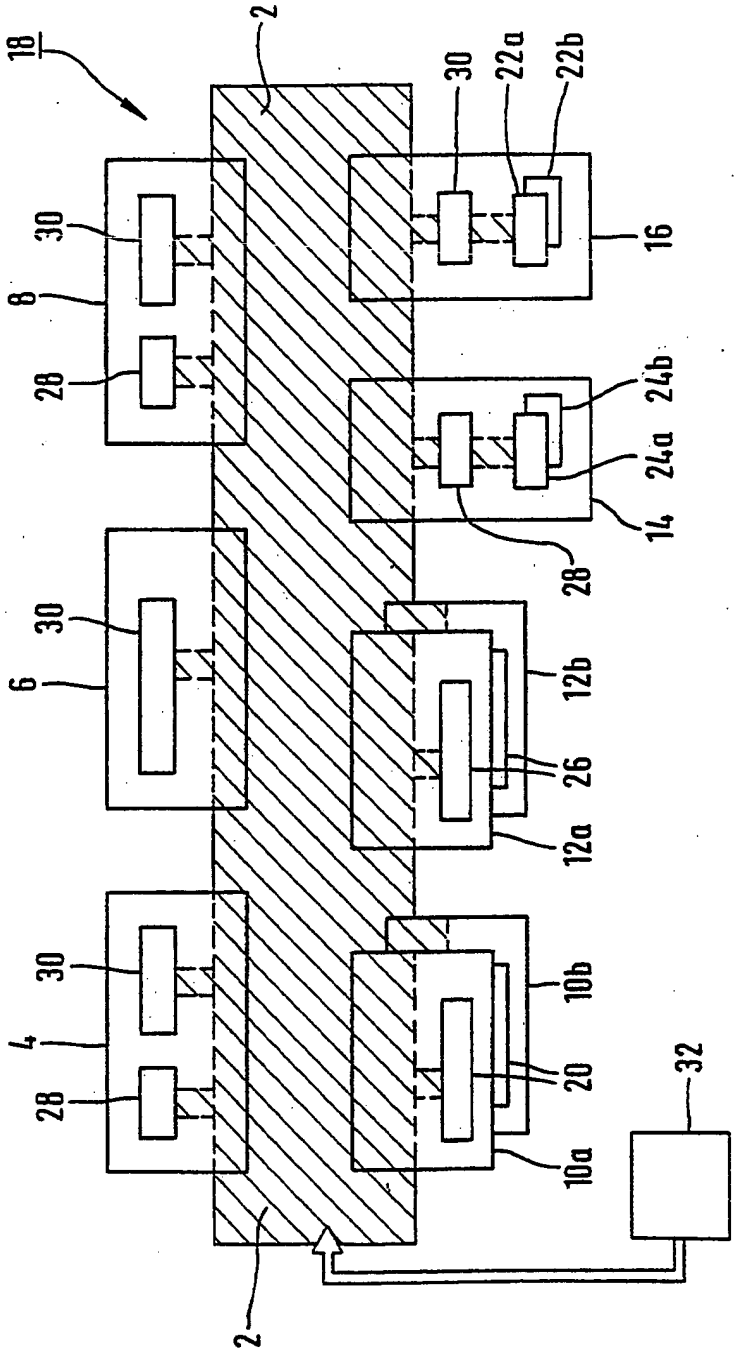


FIG 1

- Leerseite -

Nummer: DE 195 20 744 C2
Int. Cl.[6]: G 05 B 15/00
Veröffentlichungstag: 30. September 1999

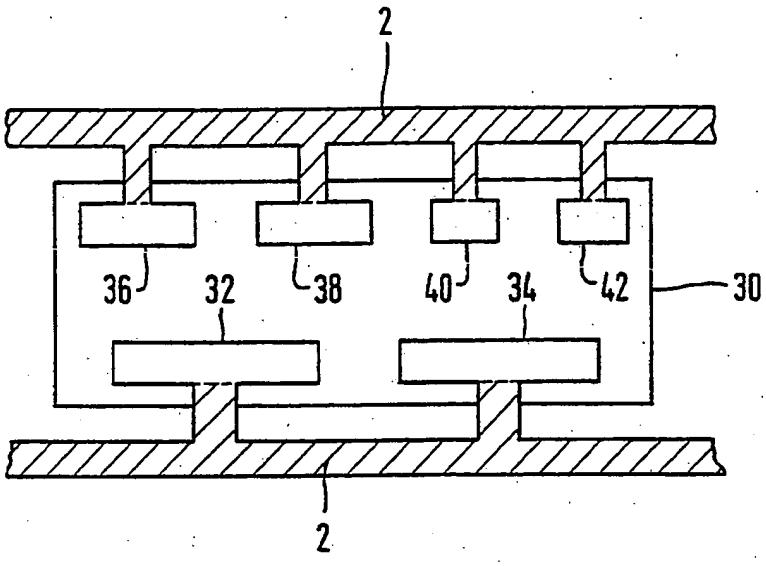


FIG 2

Nummer: DE 195 20 744 C2
Int. Cl.[6]: G 05 B 15/00
Veröffentlichungstag: 30. September 1999

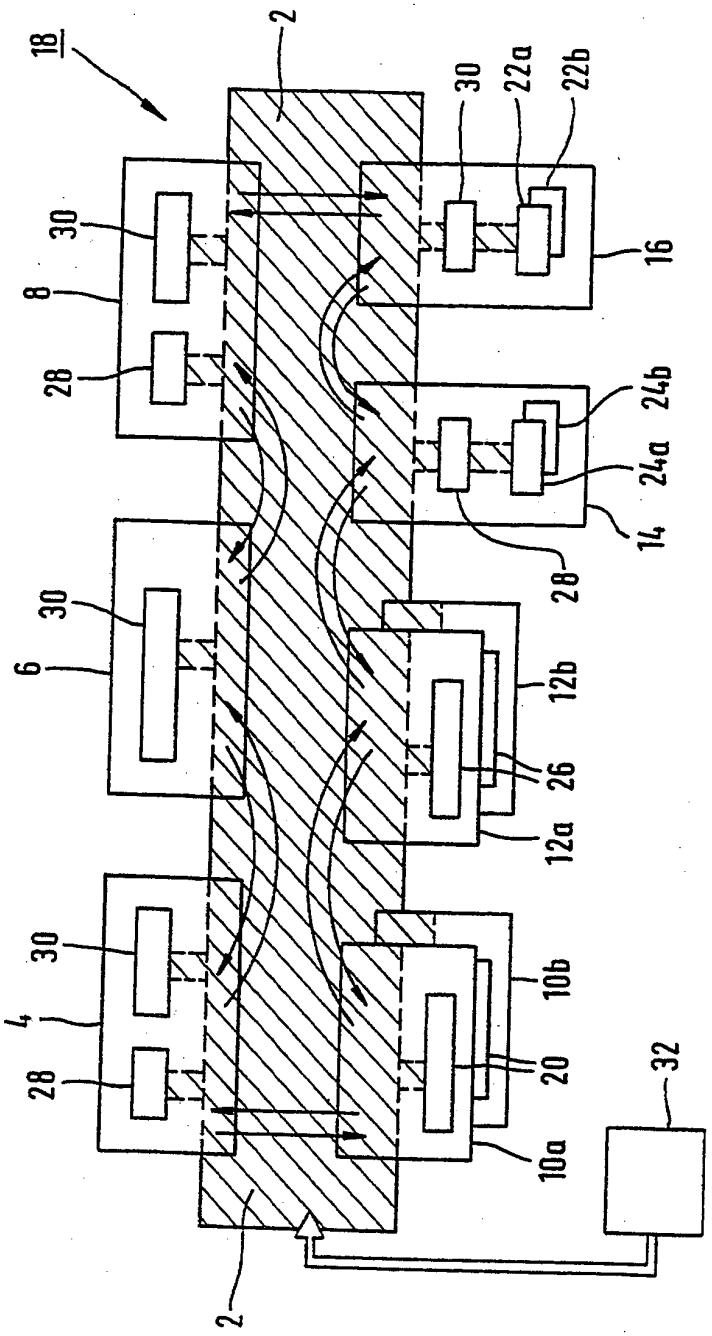


FIG 3

Nummer: DE 195 20 744 C2
Int. Cl.[6]: G 05 B 15/00
Veröffentlichungstag: 30. September 1999

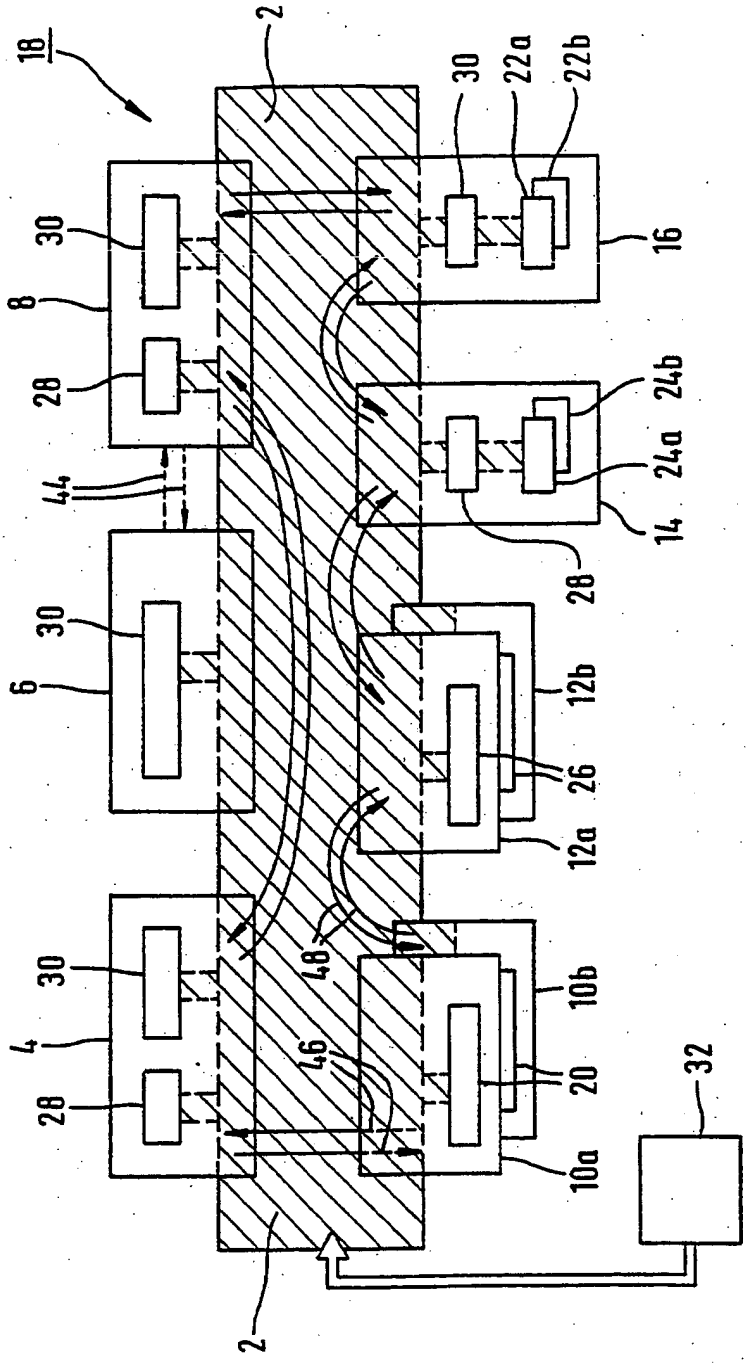


FIG 4

Nummer: DE 195 20 744 C2
Int. Cl.[6]: G 05 B 15/00
Veröffentlichungstag: 30. September 1999

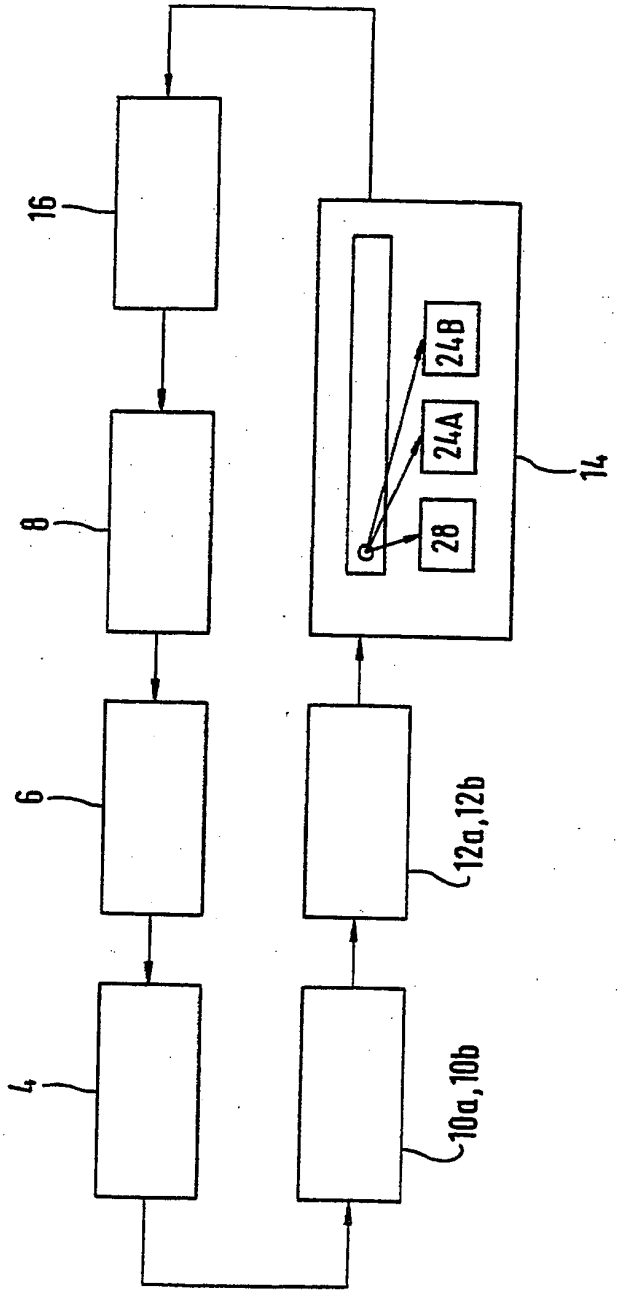


FIG 5